

Ch 5, Information Management

IMPORTANCE OF DATA AND INFORMATION TO ORGANISATIONS

Data & Information

- Data is raw, unorganised facts, figures & symbols fed to a computer during the input stage. It is ideas & concepts before they have been refined.
- Information is produced when data is manipulated into a meaningful & useful form (output). It is then used to assist decision-making.

Improving Decision-Making

Required factors for effective decision-making:

- Information sufficient & appropriate
- Information effectively communicated to decision-makers
- Information received on time

Characteristics of Information

To be able to achieve its objective of assisting in effective decision-making information must possess certain qualities or characteristics. These include:

- Completeness
- Timeliness
- Accuracy
- Unbiased
- Clarity

Completeness

It is important that all information relevant to the decision-making process be included in the output.

If the user needs to seek additional information then a report would be considered incomplete.

Timeliness

If the information is not received in time to make the best decisions then it is of no use to the decision-makers.

Sometimes a trade-off may need to be made between completeness/accuracy and timeliness.

Accuracy

Incorrect information will lead to the wrong decisions being made or problems remaining unsolved.

The data may have been accurate but the processing/manipulation can lead to inaccurate information.

Unbiased

Information can be biased for a number of reasons, sometimes deliberate, sometimes not.

Once again any bias in the information can lead to poor decision-making.

Info can become biased through sorting (alphabetically), the selection of information presented or graphics (scale and size chosen) – see p 248.

Clarity

The intended message or conclusion of a report need to be clear to the user.

Once again this can affect the effectiveness of the information and therefore the quality of the decisions made.

GOALS & OBJECTIVES OF ORGANISATIONS AND INFORMATION SYSTEMS

Strategic planning

- A process for identifying long-term goals for an organisation.
- It looks beyond the day-to-day running of an organisation and concentrates on long-term planning.
- It gives the organisation a focus or target.

Mission & Vision Statements

- These are developed once the strategic plan is completed. They establish some common goals.
- A **mission statement** explains an organisation's reason for existence.
- A **vision statement** describes an organisation as it would appear in the future.

Goals & objectives

- Every organisation should set goals to give it a focus for the future.
- A **goal** is a broad target
- An **objective** is a more specific and measureable target that will enable the goal to be achieved.

Goals & objectives

- An example of a goal may be to improve the profitability of the organisation.
- An objective to achieve this goal could be:
"To reduce costs by 15% in the next six months through more targeted purchasing decisions".

Role of Information Systems

- An **information system** is the combination of hardware & software components (digital systems), data, processes and people to create digital solutions.
- They should be designed to assist organisations achieve their goals.

Role of Information Systems

- The goal of an IS should be to make improvements in efficiency, effectiveness and decision-making.
- If the information being produced by the IS is not assisting the organisation in goal achievement, then changes need to be made.

INFORMATION MANAGEMENT STRATEGIES

Importance of information

- Information & data have become vital assets for the effective functioning of any organisation.
- Just like any other resource (staff, equipment, money) info & data can be used to support an organisation to achieve its goals.

Issues with data & information

- A number of questions can arise from the use of information:
 - ✓ How do we protect it,
 - ✓ How do we store it
 - ✓ How do we destroy it,
 - ✓ What is the correct use of it.
- For this reason policies and legislation have been developed to give organisations direction.

Maximising opportunities

Effective & efficient strategies can gain advantages through:

- reducing costs,
- support decision-making,
- encourage decisions based on actual data,
- improved forecasting / budgeting
- tailor products to customer needs/wants.

Minimising risk

Effective & efficient strategies can reduce the risk to an organisations sustainability. Risks can include:

- theft or hacking,
- loss of equipment,
- staff not following correct policies or procedures,
- destruction of data,
- legal proceedings.

Measures to minimise risk

- Keep equipment physically secure,
- Use of anti-virus & spyware protection,
- Firewalls & UPS,
- Appropriate back-up strategies,
- Password policies,
- Ensuring staff follow policies,
- Following legal obligations.

Legal obligations

- The rapid spread of electronic communications and storage systems has seen a proliferation of data being collected, stored and communicated.
- This has led to the need for laws to govern how this data is managed.
- Criminal penalties can arise from failing to adhere to the law. It can also lead to loss of reputation and trust with customers.

Privacy policies

- An organisation that collects data on individuals & other organisations usually has a privacy policy.
- The policy will disclose how the data will be collected and how it will be used. This isn't always obvious to consumers.
- By law the policy must be included on a company's website.

Key legislation for storage & disposal of data and information

Legal Obligations

Over the years a number of pieces of legislation have been introduced by both state and federal governments to govern the collection and use of private information by both government and non-government organisations.

Legal Obligations

- Organisations have a legal responsibility to ensure that these laws are implemented at the organisational level.
- Organisations also are responsible for making employees and customers aware of their rights under these laws

Information Privacy

- The rights of individuals or organisations to disallow or restrict the use of information about them.
- It has become more important due to the large amounts of personal data now being collected and stored which has increased the potential for unauthorised use.

Legislation

Key laws relating to the collection, storage and disposal of information include:

- Privacy Act 1988, amended by Privacy Amendment (Enhancing Privacy protection) Bill 2012, into effect March 2014
- Privacy and Data Protection Act 2014 (Vic)
- Health Records Act 2001 (Vic)

The Privacy Act 1988

Stipulates 13 Australian Privacy Principles that apply to the collecting, handling, accessing, using, disclosing and correcting of personal information.

Legislation covers:

- Commonwealth Government sector
- private health service providers
- private sector organisations (turnover > \$3m) and those that trade personal information.

The Privacy Act 1988

Data Collection – it must be collected in a manner that is lawful and those providing the information are informed of its intended use.

The Privacy Act 1988

Data processing, storage & maintenance:

- agencies must ensure the info is accurate, up-to-date and complete.
- individuals can access their records and request alterations.
- Information that is stored is secure and has access restricted to those who have legitimate purposes.
- Information is only kept for a timeframe that is reasonable in the context of the purpose the data was collected for.

The Privacy Act 1988

Data Use:

- Data can only be used for the purpose it was collected.
- Any other use must be accompanied by the consent of the individual it was collected from, unless there is a threat to life or health, or in the enforcement of the law
- Act applies to both electronic & manual forms of data gathering

The Privacy Act 1988

- Direct marketing via email can only be used with the consent of the individual
- Code of practice for credit reporting
- Defines personal information
- Penalties, fines of up to \$340,000 for individuals and \$1.7 M for public & private organisations

Privacy and Data Collection Act (Vic) 2014

- The act is intended to strengthen the protection of personal information and other data held by Victorian government agencies including local government bodies and contractors working for the state government.
- Scope is similar to Privacy Act, however it has its own set of Information Privacy Principles Created Commissioner for Privacy & Data protection
- Principles involve collection of information, use & disclosure, data quality & security, openness, access & correction, anonymity

Health Records Act (Vic) 2001

- Victorian Government passed this act with the intention of protecting patients medical information in both the public and private sectors.
- Establishes 11 Health Privacy Principles to provide rights to both living & deceased people in Victoria.
- Applies to the collection, use and storage of personal health information.
- Allows people to access their own medical info
- Protects confidentiality of patients health care info (except in certain extreme circumstances, an emergency, eg. Life threatened or serious threat to public health & welfare, research in public interest, investigation of unlawful activity.)

ETHICS & INFORMATION SYSTEMS

What are ethics?

- Ethics are the principles of right or wrong that are accepted by an individual or social group.
- Ethical behaviour often guides policymakers in an organisation.
- This dictates how the organisation will act in certain circumstances.

Ethical dilemmas

- An ethical dilemma occurs when there is a choice between two opinions of equal desirability.
- Examples could include:
 - ✓ freedom of expression v censorship
 - ✓ privacy v public safety
 - ✓ employee monitoring v productivity

Overcoming ethical dilemmas

In a workplace tensions over ethical issues can lead to poor productivity.

Procedures to limit the effect include:

- Ensure both employees & employers are aware of their workplace responsibilities.
- Use of codes of conduct and computer-use policies.

Steps to solving ethical dilemmas

1. Identify the problem
2. Identify the stakeholders
3. Identify possible consequences
4. Identify ethical standards
5. Evaluate options
6. Make a decision

THREATS TO DATA & INFORMATION

The need to protect info

- Organisations go to great lengths to gather and store data.
- The value of the data may vary from being merely useful, to vital to the day-to-day functioning of the organisation.
- Often its value depends on how easily it can be replaced, can the organisation function without it, or the affect if others access the data.

Consequences of poor security

The main consequences resulting from poor security are:

- Breaches of privacy legislation
- Loss of intellectual property & competitive advantage
- Loss of income due to unavailability of information or services
- Loss of public image, resulting in loss of customers

What is Security?

- Any measures that organisations take to minimize potential loss of data.
- Data and information can be damaged, destroyed, stolen, copied or deleted in multiple ways, many of which are avoidable.
- Security needs to minimize any threats whether they are deliberate, accidental and technical and event-based.

Security Procedures

- Organisations require policies to define how an information system should store, communicate & dispose of data.
- The policy should outline the procedures to be followed as well as the techniques required (physical & software controls).
- The techniques should be chosen with the efficiency and effectiveness of the info system in mind.

Accidental Threats

Usually occurs when authorised users cause damage because they are unaware of the effect of what they are doing or they lack training.

Problems also occur when proper policies and procedures are not in place, or are not followed correctly.

Many programs try to limit this damage through the use of dialogue boxes to confirm particular actions should be completed.

Examples include user error, poorly managed backups, lost data storage devices and unsafe internet usage.

Deliberate Threats

- Usually occurs due to unauthorised access to the network/system by groups or individuals seeking commercial gain, promoting causes or just being mischievous.
- It is tempting because data can be accessed remotely with little effort or risk of being detected.
- Examples include: computer viruses, hacking or cracking, information or identity theft, vandalism or theft of equipment, espionage or fraudsters.

Technical threats

Hardware or Software that stop working or fail to work as they should can cause problems such as loss of data, corrupt data or data that cannot be accessed.

These failures can be caused by:

- Equipment failure or improperly configured equipment.
- Software failure or bugs
- Variations in electricity flows
- Malware infections

Event-based threats

Natural or man-made events can threaten an organisation's data and infrastructure.

These threats can be caused by:

- Natural disasters (fire, flood, storms)
- Man-made events (terrorism, wars, riots or civil unrest)

DISASTER RECOVERY

Disaster recovery plan

Comprehensive scheme that explains how to prepare for, survive and recover from a disaster that affects information systems infrastructure.

Features include:

- prepared in advance
- tested regularly
- executed immediately
- minimizes disruption
- restores business operation as soon as possible

Disaster recovery plan

Benefits of a well designed plan are:

- provides a sense of security & confidence for management & staff,
- prevents problems that may be caused by panic,
- reduces uncertainty and pressure on decision-makers,
- explains procedures to staff.

Disaster recovery plan

To be prepared for a disaster a lot of work must be completed beforehand to be ready. This is the scope of the plan.

- Risk assessment – probability & consequences of different risks.
- Allocating emergency responsibilities (including secondary if people are absent)
- Auditing all equipment so replacements can be quickly accessed.
- Key information is documented and located for easy access

Backing up

A DRP must outline an effective data backup scheme.

It should specify how and when backups are done, and by whom.

This involves the choice of a backup scheme and backup media.

Backup scheme

Common types of backup schemes:

- Daily incremental – only saves changes from previous day. Quick and uses little space.
- Weekly full – used in conjunction with daily incremental.
- Differential – saves all changes since last **full** backup (not last incremental).
- Partial – only backs up selected areas.

Backup media

Common types of backup media:

- Tape
- External HDD
- Online, cloud
- CD/DVD
- USB flash drive

Storage off-site is important. Automated systems that carry out data duplication can be an effective option.

Testing the backup scheme

- It is not sufficient (or recommended) that it is just assumed that backed up data will be able to be restored efficiently (quickly) and effectively (complete & accurate).
- Because systems are regularly changed it is vital that backup schemes are regularly tested.
- They need to be tested to see if they are still saving the correct data and can be retrieved in case of an emergency.

Testing the DRP

The four main components of a DRP are:

- Evacuation
- Backing up data
- Data restoration
- **Testing of disaster recovery plan**

In many ways this last step is the most important. Waiting to see if the plan works could be disastrous.

Practicing evacuation, backing up and restoration procedures ensure that they are appropriate and effective. Hopefully the disaster never occurs.

Information Systems

What is a System?

A system is a group of components that work together.

Examples include:

- a farming system (running a local farm)
- an education system (Charlton College)
- a business system (a supermarket)

What is a System?

Whatever the system it always has three main steps.



- **Input** – the raw materials, equipment, personnel etc that are placed into the system.
- **Process** – the activities and procedures used to manipulate and convert the inputs.
- **Output** – the final product of the system.

List what the inputs, processes and outputs would be for a farm and a bakery.

What is an Information System?

An information system is just one type of system. What sets it apart is that the inputs are data while the output is information.

- **Data:** raw, unprocessed, unorganised facts and figures. An examples could be a bundle of survey sheets.
- **Information:** data that has been manipulated or organised into a meaningful and useful form. An example could be the results of a survey presented as a graph.

What is an Information System?

The basic information system would work as follows:

- **Input:** this is the entering of the raw data into a computer application, eg: enter the results of a survey into a spreadsheet.
- **Process (manipulate):** this is the use of the application to organise and manipulate the data into a useful form (information), eg: using the spreadsheet to create a graph.
- **Output:** the actual information in a useful form, eg: a printout of the graphs.

Information Systems

Why does an organisation need an information system:

- to process, manage & protect data
- assists in decision-making
- helps control the activities of the business
- allows an organisation to achieve its overall goals and objectives

Components of an Information System

There are five basic components of an information system:

- People
- Processes
- Data
- Digital systems

People

Two basic groups of people are involved in information systems:

- IS providers who set up and maintain the system (technical support, system analysts, software & web developers, system & network managers)
- IS users who use the system to assist the in completing their prime function (eg: teachers, managers, customers). They may not actually use the equipment, but rely on the information produced (eg: reports).

Processes

In an IS these would include acquisition, input, validation, manipulation, storage, retrieval, output, communication & disposal.

The organisation should stipulate, through policies & manuals, the most efficient and effective methods of completing the tasks.

By following the correct procedures it ensures that the tasks are performed uniformly and consistently.

Data

As discussed earlier data is entered into the information system to begin the process.

Some points about data:

- data is raw and unorganised.
- it may be in the form of letters, numbers, images or sounds.
- for it to become meaningful it needs to be processed or manipulated.

Digital systems

This is the equipment used within an information system.

- Hardware is the physical computer equipment.
- Software are computer programs that direct the computer what to do.
- Networks is made up of computers & devices connected by communication channels that facilitate communication and sharing of resources between users.

Types of Hardware

- **Input devices** – the equipment used to enter the data such as keyboards, mouse, microphones and cameras.
- **Output devices** – the equipment that allows the output of the system to be communicated to the users such as monitors, printers, data projectors and speakers
- **System unit** – the brain of the computer situated in the main “box”. Includes CPU and motherboard.
- **Storage devices** – site where the info is stored such as hard drives, DVDs, flash drives.
- **Communication devices** – items that allow communication with other computers (modem, NIC’s).

Types of Software

- **System Software** – manages the operation of the computer (both hardware & software) eg: Windows
- **Application Software** – allows specific types of processing eg: Excel, Word
- **Utility Software** – management of certain aspects such as disks eg: anti-virus programs, converting file formats, capturing screen shots.

Networks

Advantages:

- Share data easily (and instantaneously),
- Share resources (printers, storage devices, software),
- Assists collaboration (file versioning).

Disadvantages:

- Equipment failure affects entire network.

The Cloud

- Any internet based software and data storage facility.
- Includes online services that carry out processing on the user's behalf.
- Examples of services include: email, application software (word processing & spreadsheets), forms for data collection, data visualisations, calendars, project management & games.

The Cloud

Advantages:

- Improved mobility (anytime, anywhere),
- Collaboration improved (globally),
- Less setup, maintenance & upgrade costs,
- Security is outsourced,
- Easily recoverable (especially after a disaster)

Disadvantages:

- Require internet connection,
- Access can be slow & expensive (depends on connection),
- Placing trust in third party provider.

EVALUATING INFORMATION MANAGEMENT STRATEGIES

Evaluation

- This presentation refers to how to evaluate the strategies chosen for different components of an information system.
- It could include evaluating:
 - ✓ backup schemes
 - ✓ hardware & software components
 - ✓ different procedures (work practices)

Evaluation

- It is important to distinguish between evaluation & testing.
- Testing is conducted to ensure the strategy functions how it was designed.
- Evaluation checks that the strategy is achieving the goals and objectives for which it was designed.
- Criteria are set to assess this.

Evaluating strategies

- When using different strategies it is always important to assess whether they have been effective – have they achieved their goals and objectives.
- Criteria should be stated that evaluate the solutions requirements - functional (does it work) and non-functional (ease of use).

Evaluating strategies

- It is important that the criteria are monitored over a period of time, and that this monitoring is recorded so that the strategy can be successfully evaluated.
- Evaluation criteria generally fall under the categories of efficiency or effectiveness.

Evaluating effectiveness

Effectiveness criteria measure the **quality** of the strategy – how well it performs. This would include:

- Integrity of data,
- Security,
- Ease of retrieval,
- Currency of files

Evaluating efficiency

Efficiency criteria measure the **processes** of the strategy. This would include:

- Time (speed),
- Cost,
- Effort.